

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor : RUMP, Neils
Application No. : 09/913,686
Patent No. : 7,434,052
Issue Date : October 07, 2008
Art Unit : 2131
Confirmation Number : 3745
Examiner : Henning, Matthew T.
Title : Method and Device for Producing an
Encrypted Payload Data Stream and Method
and Device for Decrypting an Encrypted
Payload Data Stream
Attorney Docket No. : SCHO0093

November 07, 2008

Commissioner of Patents and Trademarks
Mail Stop: Certificate of Corrections Branch
P.O. Box 1450
Alexandria, VA. 22313-1450

REQUEST FOR CERTIFICATE OF CORRECTION UNDER 37 CFR § 1.322

The enclosed Certificate of Correction (PTO/SB/44) for the above-identified patent is submitted under 37 CFR § 1.322.

Applicant requests the following correction be made:

CHANGE Section (75)

FROM 'Inventor: Niels Rump, Kent (GB)'
TO 'Inventors: **Niels Rump**, Kent (GB);
Juergen Koller, Erlangen (DE); and
Karlheinz Brandenburg, Erlangen (DE)'

See attached Declarations and Filing Receipt for verification that the above information is correct.

The correction does not involve such changes in the patent as would constitute new matter or would require reexamination as set forth in 35 U.S.C. § 254. Therefore, no new matter is provided with this Certificate of Correction.

The Commissioner is hereby authorized to charge the fee set forth in 37 CFR § 1.20(a) and any additional fees due, to Deposit Account 07-1445 (Order No. SCHO0093).

Respectfully submitted,

A handwritten signature in black ink, appearing to be 'Michael A. Glenn', with a long horizontal stroke extending to the right.

Michael A. Glenn
Reg. No. 30,176

Customer No. 22862

UNITED STATES PATENT AND TRADEMARK OFFICE CERTIFICATE OF CORRECTION

Page 1 of 1

PATENT NO. : 7,434,052
APPLICATION NO.: 09/913,686
ISSUE DATE : October 07, 2008
INVENTOR(S) : Niels RUMP; Juergen KOLLER; and Karlheinz BRANDENBURG

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

(75) Inventors: Niels Rump, Kent (GB);
Juergen Koller, Erlangen (DE); and
Karlheinz Brandenburg, Erlangen (DE)

MAILING ADDRESS OF SENDER (Please do not use customer number below):

GLENN PATENT GROUP
3475 EDISON WAY, SUITE L
MENLO PARK, CA 94025

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



US007434052B1

(12) **United States Patent**
Rump

(10) **Patent No.:** **US 7,434,052 B1**

(45) **Date of Patent:** **Oct. 7, 2008**

(54) **METHOD AND DEVICE FOR PRODUCING
AN ENCRYPTED PAYLOAD DATA STREAM
AND METHOD AND DEVICE FOR
DECRYPTING AN ENCRYPTED PAYLOAD
DATA STREAM**

FOREIGN PATENT DOCUMENTS

DE 196 25 635 C1 12/1997

(75) Inventor: **Niels Rump**, Kent (GB)

(Continued)

(73) Assignee: **Fraunhofer-Gesellschaft zur
Foerderung der angewandten
Forschung e.V.**, Munich (DE)

OTHER PUBLICATIONS

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

Schneier, Bruce "Applied Cryptography Second Edition" John Wiley and Sons, pp. 30-31 and 53-54.*

(Continued)

(21) Appl. No.: **09/913,686**

(22) PCT Filed: **Dec. 15, 1999**

Primary Examiner—Ayaz Sheikh

Assistant Examiner—Matthew T. Henning

(86) PCT No.: **PCT/EP99/09981**

(74) Attorney, Agent, or Firm—Glenn Patent Group; Michael A. Glenn

§ 371 (c)(1),
(2), (4) Date: **Jan. 24, 2002**

(57) **ABSTRACT**

(87) PCT Pub. No.: **WO00/49763**

PCT Pub. Date: **Aug. 24, 2000**

(30) **Foreign Application Priority Data**

Feb. 16, 1999 (DE) 199 06 450

(51) **Int. Cl.**
H04L 9/08 (2006.01)
H04L 9/30 (2006.01)
H04L 9/16 (2006.01)

(52) **U.S. Cl.** **713/171; 713/160; 713/161;
380/45; 380/260; 380/261; 380/284**

(58) **Field of Classification Search** **380/45,
380/284, 260-261; 713/160-161, 201, 171**
See application file for complete search history.

(56) **References Cited**

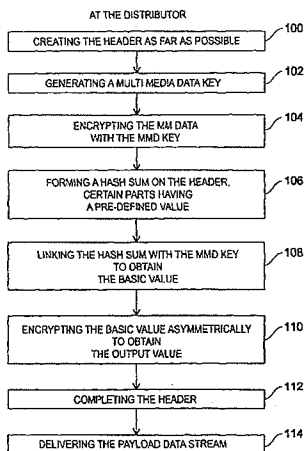
U.S. PATENT DOCUMENTS

4,899,333 A * 2/1990 Roediger 370/427

(Continued)

In a method for producing an encrypted method payload data stream comprising a header and a block containing encrypted payload data, a payload data key for a payload data encryption algorithm for encrypting payload data is generated. The payload data is encrypted using the generated payload data key and the payload data encryption algorithm to obtain the block containing the encrypted payload data of the payload stream. A part of the payload data stream is processed to deduce information marking the part of the payload data stream. The information is linked with the payload data by means of an invertible logic linkage to obtain a basic value. This basic value is finally encrypted using a key of two keys being different from each other by an asymmetrical encryption method, the two different keys being the public and the private keys respectively for the asymmetrical encryption method to obtain an output value being an encrypted version of the payload data key. The output value is finally entered into the header to complete the payload stream. Changes of the header and of the payload data itself, which are not authorized, lead to an automatic destruction of the payload data.

30 Claims, 4 Drawing Sheets





COMBINED DECLARATION AND POWER OF ATTORNEY

**(ORIGINAL, DESIGN, NATIONAL STAGE OF PCT, SUPPLEMENTAL, DIVISIONAL,
CONTINUATION, OR C-I-P)**

As a below named inventor, I hereby declare that:

TYPE OF DECLARATION

This declaration is for a national stage of PCT application.

INVENTORSHIP IDENTIFICATION

My residence, post office address and citizenship are as stated below, next to my name. I believe that I am an original, first and joint inventor of the subject matter that is claimed, and for which a patent is sought on the invention entitled:

TITLE OF INVENTION

METHOD AND DEVICE FOR PRODUCING AN ENCRYPTED PAYLOAD DATA STREAM AND
METHOD AND DEVICE FOR DECRYPTING AN ENCRYPTED PAYLOAD DATA STREAM

SPECIFICATION IDENTIFICATION

The specification was filed on August 16, 2001, as Serial No. 09/913,686.

ACKNOWLEDGMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information, which is material to patentability as defined in 37, Code of Federal Regulations, Section 1.56, and which is material to the examination of this application, namely, information where there is a substantial likelihood that a reasonable Examiner would consider it important in deciding whether to allow the application to issue as a patent.

PRIORITY CLAIM (35 U.S.C. Section 119(a)-(d))

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed.

Such applications have been filed as follows.

**PRIOR PCT APPLICATION(S) FILED WITHIN 12 MONTHS
(6 MONTHS FOR DESIGN) PRIOR TO THIS APPLICATION
AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. SECTION 119(a)-(d)**

INDICATE IF PCT	APPLICATION NUMBER	DATE OF FILING DAY, MONTH, YEAR	PRIORITY CLAIMED UNDER 35 U.S.C. SECTION 119
PCT	PCT/EP99/09981	15 December 1999	yes

**PRIOR FOREIGN APPLICATION(S) FILED WITHIN 12 MONTHS
(6 MONTHS FOR DESIGN) PRIOR TO THIS APPLICATION
AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. SECTION 119(a)-(d)**

COUNTRY	APPLICATION NUMBER	DATE OF FILING DAY, MONTH, YEAR	PRIORITY CLAIMED UNDER 35 U.S.C. SECTION 119
Germany	19906450.4	16 February 1999	yes

POWER OF ATTORNEY

I hereby appoint the practitioner(s) associated with the Customer Number provided below to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Customer No. 24283

SEND CORRESPONDENCE TO:
Customer No. 24283

DIRECT TELEPHONE CALLS TO:
Carl A. Forest
303-379-1114

DECLARATION

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURE(S)

Niels Rump

Inventor's signature

Date 2002-03-19

Residence Kent United Kingdom

Post Office Address 16 Chatsworth Avenue, Bromley, Kent BR1 1DP United Kingdom

Country of Citizenship Germany

COMBINED DECLARATION AND POWER OF ATTORNEY

**(ORIGINAL, DESIGN, NATIONAL STAGE OF PCT, SUPPLEMENTAL, DIVISIONAL,
CONTINUATION, OR C-I-P)**

As a below named inventor, I hereby declare that:

TYPE OF DECLARATION

This declaration is for a national stage of PCT application.

INVENTORSHIP IDENTIFICATION

My residence, post office address and citizenship are as stated below, next to my name. I believe that I am an original, first and joint inventor of the subject matter that is claimed, and for which a patent is sought on the invention entitled:

TITLE OF INVENTION

METHOD AND DEVICE FOR PRODUCING AN ENCRYPTED PAYLOAD DATA STREAM AND
METHOD AND DEVICE FOR DECRYPTING AN ENCRYPTED PAYLOAD DATA STREAM

SPECIFICATION IDENTIFICATION

The specification was filed on August 16, 2001, as Serial No. 09/913,686

ACKNOWLEDGMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information, which is material to patentability as defined in 37, Code of Federal Regulations, Section 1.56, and which is material to the examination of this application, namely, information where there is a substantial likelihood that a reasonable Examiner would consider it important in deciding whether to allow the application to issue as a patent.

PRIORITY CLAIM (35 U.S.C. Section 119(a)-(d))

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed.

Such applications have been filed as follows.

**PRIOR PCT APPLICATION(S) FILED WITHIN 12 MONTHS
(6 MONTHS FOR DESIGN) PRIOR TO THIS APPLICATION
AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. SECTION 119(a)-(d)**

INDICATE IF PCT	APPLICATION NUMBER	DATE OF FILING DAY, MONTH, YEAR	PRIORITY CLAIMED UNDER 35 U.S.C. SECTION 119
PCT	PCT/EP99/09981	15 December 1999	yes

**PRIOR FOREIGN APPLICATION(S) FILED WITHIN 12 MONTHS
(6 MONTHS FOR DESIGN) PRIOR TO THIS APPLICATION
AND ANY PRIORITY CLAIMS UNDER 35 U.S.C. SECTION 119(a)-(d)**

COUNTRY	APPLICATION NUMBER	DATE OF FILING DAY, MONTH, YEAR	PRIORITY CLAIMED UNDER 35 U.S.C. SECTION 119
Germany	19906450.4	16 February 1999	yes

POWER OF ATTORNEY

I hereby appoint the practitioner(s) associated with the Customer Number provided below to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Customer No. 24283

SEND CORRESPONDENCE TO:
Customer No. 24283

DIRECT TELEPHONE CALLS TO:
Carl A. Forest
303-379-1114

DECLARATION

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURE(S)

Niels Rump

Inventor's signature _____


Date _____ Country of Citizenship Germany

Residence Erlangen Germany

Post Office Address Brueckenstrasse 13, Erlangen D-91056 Germany

Juergen Koller

Inventor's signature _____


Date September 24, 2001  Country of Citizenship Germany

Residence Erlangen Germany

Post Office Address St. Johann 6/113, Erlangen D-91054 Germany

Karlheinz Brandenburg

Inventor's signature _____

Date September 24, 2001  Country of Citizenship Germany

Residence Erlangen Germany

Post Office Address Haagstrasse 32, Erlangen D-91054 Germany



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
09/913,686	01/24/2002	2131	1268	SCHO0093	31	4

CONFIRMATION NO. 3745

GLENN PATENT GROUP
3475 Edison Way
Suite L
Menlo Park, CA94025

CORRECTED FILING RECEIPT

Date Mailed: 07/03/2007

Receipt is acknowledged of this regular Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please mail to the Commissioner for Patents P.O. Box 1450 Alexandria Va 22313-1450. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).**

Applicant(s)

Niels Rump, Erlangen, GERMANY;
Juergen Koller, Erlangen, GERMANY;
Karlheinz Brandenburg, Erlangen, GERMANY;

Power of Attorney:

Michael Glenn--30176
Donald Hendricks--40355
Kirk Wong--43284
Christopher Peil--45005
Julia Thomas--52283

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/EP99/09981 12/15/1999

Foreign Applications

GERMANY 199 06 450.4 02/16/1999

If Required, Foreign Filing License Granted: 07/02/2007

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is
US09/913,686

Projected Publication Date: None, application is not eligible for pre-grant publication

Non-Publication Request: No

Early Publication Request: No

Title

Method and device for producing an encrypted payload data stream and method and device for decrypting an encrypted payload data stream

Preliminary Class

713

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER**Title 35, United States Code, Section 184****Title 37, Code of Federal Regulations, 5.11 & 5.15****GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date

thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).